

Clean Version Of The Pending Claims Under 37 C.F.R. §1.121(c)(3):

In accordance with 37 C.F.R. §1.121(c)(3), claims 3-4, 6-12, and 15-22 are submitted below as a clean version of the entire set of pending claims in this single amendment paper. In addition, a marked up version of amended claims 3-4, 6-9, and 15-17, showing all the changes relative to the previous version of these claims, is submitted on one or more pages separate from this amendment in accordance with 37 C.F.R. §1.121(c)(3).

1. (Canceled)

2. (Canceled)

3. (Amended) A computerized method for key-based secure storage comprising:

downloading information and an access predicate that specifies requirements for an application to access the information;

generating a seed value;

producing a hash seed value based on the seed value using a one-way hash function;

generating an application storage key from the hash seed value;

encrypting the information using the application storage key; and

associating the access predicate with the encrypted information.

1 (Amended) A computerized method for key-based secure storage
2 comprising:

3 downloading information and an access predicate that specifies
4 requirements for an application to access the information;

5 generating a seed value;

6 producing a first hash seed value based on the seed value using a one-way
7 hash function;

8 producing a second hash seed value based on the seed value and a user
9 identifier using a keyed hash function;

10 generating a user storage key from the second hash seed value;

11 encrypting the information using the user storage key; and

12 associating the access predicate with the encrypted information.

13
14 [5. (Canceled)]

15
16 3. (Amended) A computerized method for key-based secure storage
17 comprising:

18 downloading information and an access predicate that specifies
19 requirements for an application to access the information;

20 obtaining a storage key;

21 encrypting the information using the storage key;

22 associating the access predicate with the encrypted information;

23 obtaining an operating system storage key;

24 encrypting the access predicate with the operating system storage key; and
25

1 encrypting a plurality of other storage keys using the operating system
2 storage key, wherein the other storage keys are selected from the group consisting
3 of application storage keys and user storage keys.

4
5 ⁴
6 ~~7.~~ (Amended) A computerized method for key-based secure storage
7 comprising:

8 downloading information and an access predicate that specifies
9 requirements for an application to access the information;

10 obtaining a storage key;

11 encrypting the information using the storage key;

12 associating the access predicate with the encrypted information;

13 generating a seed value;

14 generating an operating system storage key based on the seed value; and

15 encrypting the access predicate with the operating system storage key.

16 ⁵
17 ~~8.~~ (Twice Amended) A computerized method for key-based secure
18 storage comprising:

19 downloading information and an access predicate that specifies
20 requirements for an application to access the information;

21 generating a seed value for the application;

22 producing an application hash seed value based on the seed value for the
23 application using an application-specific one-way hash function;

24 generating an application storage key from the application hash seed value;

25 generating a seed value for a user;

1 producing a first user hash seed value based on the seed value for the user
2 using a one-way hash function;

3 producing a second user hash seed value based on the first user hash seed
4 value and a user identifier using a keyed hash function;

5 generating a user storage key from the second user hash seed value, the
6 application storage key and the user storage key to encrypt information containing
7 a portion specific to an application and a portion specific to the user;

8 encrypting the information using the application storage key and the user
9 storage key; and

10 associating the access predicate with the encrypted information.

~~11~~ ~~12~~ ⁶ ~~9.~~ (Amended) A computerized method for key-based secure storage
13 comprising:

14 downloading information and an access predicate that specifies
15 requirements for an application to access the information;

16 obtaining a storage key;

17 encrypting the information using the storage key;

18 associating the access predicate with the encrypted information;

19 storing the storage key in a key vault provided by a third-party; and

20 recovering the storage key from the key vault.

~~21~~ ⁷ ~~10.~~ The computerized method of claim ⁶ ~~9~~, wherein recovering the storage
22 key comprises:

23 requesting recovery of the storage key; and

24 providing information to the third-party to enable validation of the request.
25

B

1
2 ~~11.~~ ⁶ The computerized method of claim ~~9~~, further comprising:
3 selecting the key vault from a plurality of key vaults provided by a trusted
4 operating system.

5
6 ~~12.~~ ⁹ The computerized method of claim ~~9~~, further comprising:
7 selecting the key vault designated by a provider of the information.

8
9 [13. (Canceled)]

10
11 [14. (Canceled)]

12
13 ~~15.~~ ¹⁰ (Amended) A computer system comprising:
14 a processing unit;
15 a system memory coupled to the processing unit through a system bus;
16 a computer-readable medium coupled to the processing unit through a
17 system bus;
18 a generate key function executed from the computer-readable medium by
19 the processing unit, wherein the generate key function causes the processing unit
20 to generate an operating system storage key based on an identity for the operating
21 system and based on a seed.

22 11

23 ~~16.~~ (Amended) A computer system comprising:

24 a processing unit;

25 a system memory coupled to the processing unit through a system bus;

1 a computer-readable medium coupled to the processing unit through a
2 system bus;

3 a generate key function executed from the computer-readable medium by
4 the processing unit, wherein the generate key function causes the processing unit
5 to generate an operating system storage key based on an identity for the operating
6 system;

7 an application specific one-way hash function executed from the
8 computer-readable medium by the processing unit, wherein the application
9 specific one-way hash function causes the processing unit to generate an
10 application storage key from a hashed seed; and

11 a generate application key function executed from the computer-readable
12 medium by the processing unit, wherein the generate application key function
13 causes the processing unit to generate the hashed seed from an application seed.

14
15 ¹²
~~17.~~ (Amended) A computer system comprising:

16 a processing unit;

17 a system memory coupled to the processing unit through a system bus;

18 a computer-readable medium coupled to the processing unit through a
19 system bus;

20 a generate key function executed from the computer-readable medium by
21 the processing unit, wherein the generate key function causes the processing unit
22 to generate an operating system storage key based on an identity for the operating
23 system;

1 a key-hash function executed from the computer-readable medium by the
2 processing unit, wherein the key-hash function causes the processing unit to
3 generate a user storage key from a hashed seed and an identity for the user;

4 a one-way hash function executed from the computer-readable medium by
5 the processing unit, wherein the one-way hash function causes the processing unit
6 to generate the hashed seed from a previously hashed seed; and

7 a generate user key function executed from the computer-readable medium
8 by the processing unit, wherein the generate user key function causes the
9 processing unit to generate the previously hashed seed from a user seed.

10 ¹³

11 ~~18.~~ A computer system comprising:

12 a processing unit;

13 a system memory coupled to the processing unit through a system bus;

14 a computer-readable medium coupled to the processing unit through a
15 system bus; and

16 a trusted operating system executed from the computer-readable medium by
17 the processing unit, wherein the trusted operating system causes the processing
18 unit to encrypt downloaded information using a storage key based on a seed
19 value.

20 ¹⁴

21 ~~19.~~ The computer system of claim ¹³ ~~18~~, wherein the trusted operating
22 system further causes the processing unit to encrypt an access predicate associated
23 with the downloaded information using an operating system storage key, to
24 encrypt the seed value for the storage key using the operating system storage key,
25 and to associate the encrypted access predicate with the encrypted seed value.